Welcome! Please follow these instructions

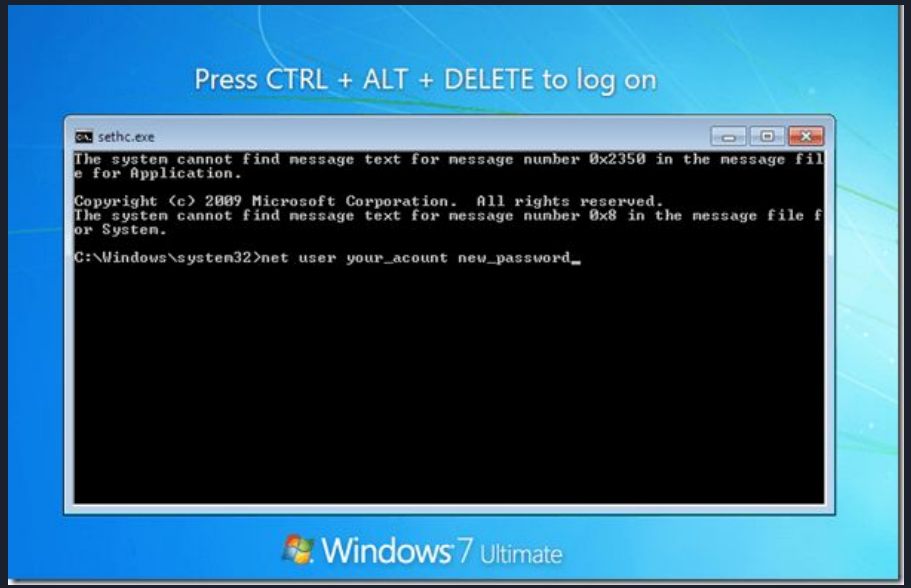
1. Either grab a lab pc, or on your own pc connect to Big Koala (password = putinattackhelicopter)
2. Go to 10.1.1.132
3. Make an account
4. The meeting will begin shortly!

Hacking Windows Systems

By Derek and Stanley

SYSTEM Shell on Winlogon Desktop

1. Live boot into another OS such as kali
2. Make a copy of c:\windows\system32\cmd.exe
3. Make a backup copy of c:\Windows\System32\sethc.exe
4. Replace original sethc.exe with the copy of cmd.exe
5. Boot windows up
6. Hit shift a bunch of times
7. HACKED



Adding an Admin account

Run the following commands to make a new account and add it to the administrators group:

- net user hacker abcd /add
- net localgroup administrators hacker /add

Cracking Windows Passwords

Passwords are stored in hashes in the following file:

C:\windows\system32\config\sam

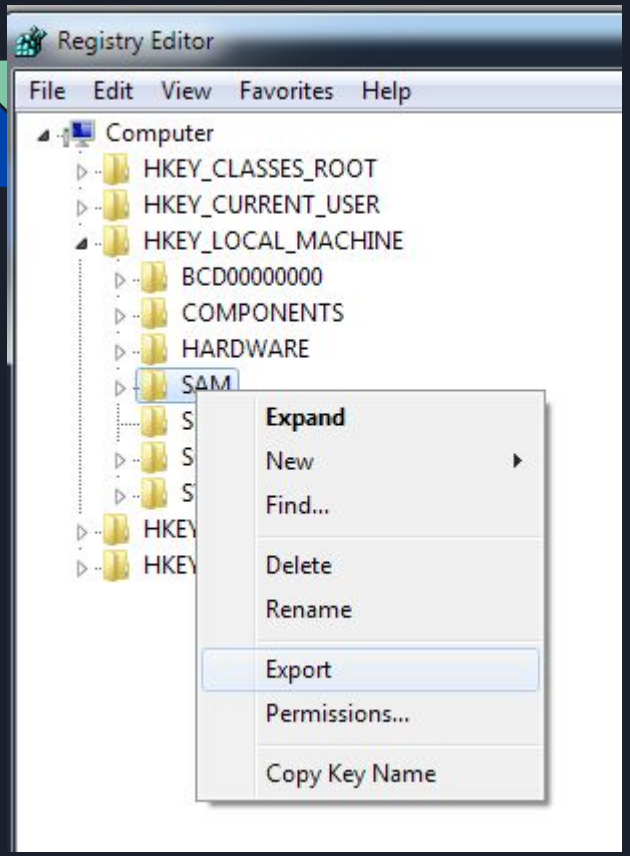
The hashes are encrypted with a key stored in another file:

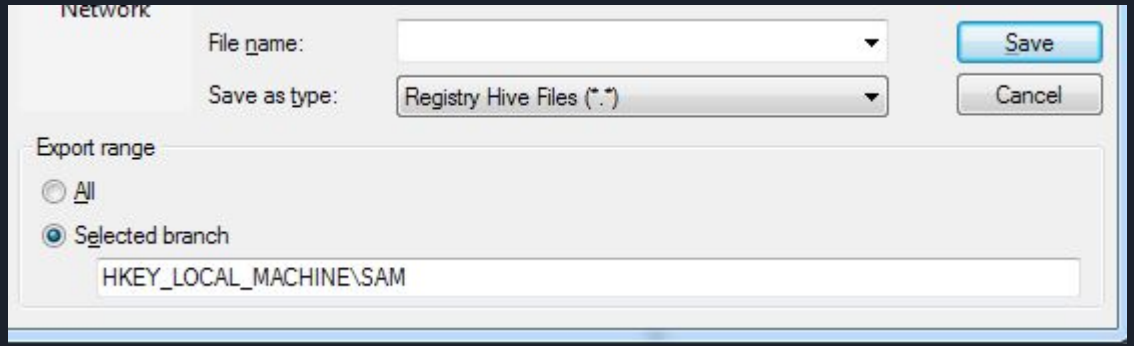
C:\windows\system32\config\security

Both files are required to obtain the hashes

Cracking Windows Passwords

- Both of these files are protected by the OS so cannot be copied directly.
- But they can be obtained using the registry utilities reg or regedit if you have administrative privileges
- Reg is a command line utility and the commands are as follows:
  - REG SAVE HKLM\Sam c:\sam
  - REG SAVE HKLM\System c:\System
- Regedit is a GUI
- Open it up and expand HKEY_LOCAL_MACHINE
- Right click on SAM and click export
- Change the file type to Registry Hive Files
- Repeat this for SYSTEM


Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
COMPONENTS
HARDWARE
SAM
Expand
New
Find...
Delete
Rename
Export
Permissions...
Copy Key Name


Network
File name:
Save as type:
Registry Hive Files (*.*)
Save
Cancel
Export range
All
Selected branch
HKEY_LOCAL_MACHINE\SAM

Extracting the Hashes

- There’s a few tools to do this.
- Pwdump7 and Cain and Abel are the two I use.
- Pwdump7 was having issues on the vm so we’ll use cain and abel
- Download it from oxid.it
- Install it. Make sure to hit yes when it asks to install pcap drivers
- Go to the cracker tab and click LM & NTLM hashes on the left
- Click the plus button to import
- Select the SAM file
- To get the boot key, click the … button then click the second … button and select the SYSTEM file
- Copy and paste the boot key into the text box

Extracting the Hashes

- The hashes should now be displayed in the cracker window
- Right click and hit export
- Save the file and then open it with notepad
- You should see lines that look like this
- Administrator:"":"":AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
- The colons serve as delimiters and the format is as following
- Username:::LM Hash:NTLM Hash
- If the LM Hash is AAD3B435B51404EEAAD3B435B51404EE (empty hash) that means the password is only stored as an NT hash
- LM Hashes are literally a joke to crack, so if it's not the hash mentioned above, you hit the jackpot!

LM Hashes

AAD3B435B51404EEAAD3B435B51404EE
AAD3B435B51404EEA AD3B435B51404EE

AAD3B435B51404EE
AAD3B435B51404EE

- LM hashes are really two hashes appended to each other
- Each hash supports a max of 7 characters (for a max length of 14 characters)
- The password is converted to uppercase before being hashes
- So yes, its a joke and can be cracked in a couple minutes

NT Hashes

- Not a joke like LM
- All systems starting with Vista / Server 2008 have LM hashes disabled by default and only use NT hashes

Cracking

- Tons of tools available to crack hashes
- Some common tools are Hashcat, John the Ripper, Cain and Abel, and Ophcrack
- The premise of cracking is taking a potential password, computing the hash of it, and comparing it to the hash you have
- Three main methods of cracking:
  - Dictionary / Wordlist
  - Bruteforce
  - Rainbow Tables
- Dictionaries are lists of passwords to try
- Brute forcing generates passwords following a set of rules. Ex. 1-8 characters a-z
- Rainbow tables are tables with precomputed hashes from either bruteforce or dictionaries. The tables are then searched for the target hash. This is the fastest hash cracking method

Cracking - The lazy way

- There’s also online crackers that you can just put the hash into
- I always try this first because its super easy and has a decent success rate
- The two I generally use are
  - https://crackstation.net/
  - https://hashkiller.co.uk/ntlm-decrypter.aspx
- So now that we have the hashes, grab the NT hash from the Bichael account and paste it into one of the online crackers
- We should get the password in a couple seconds

Fun information

- Now that we have the password to Bichael - log into the account
- We’re going to find his passwords for websites and some hidden embarrassing photos

Chrome Forensics

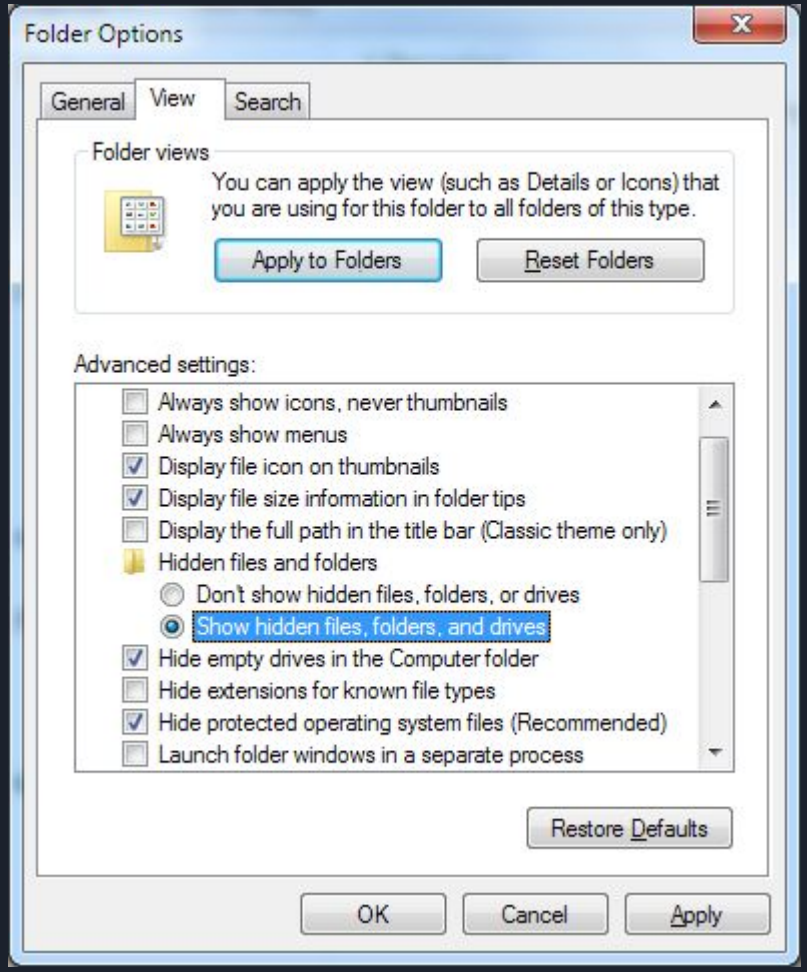
- Press CTRL+H to bring up the browser history
- We can see that Bichael has been do the dominos website
- Lets go there!

Chrome Forensics

- We can also see that he has his credentials saved - lets get them
- Download chromepass from https://www.nirsoft.net/utils/chromepass.html
- Run it and we should now have his passwords
- Now we can order pizza under his name >:)
- (We can also get the passwords by using the builtin chrome password manager, but chromepass gets them all in one sweep)

Super hidden files

- On the desktop, there is a folder containing embarrassing photos
- Its hidden obviously, so let's try and show it
- Open a file explorer window, hit ALT to show the toolbar, then goto Tools -> Folder options
- Select Show Hidden files

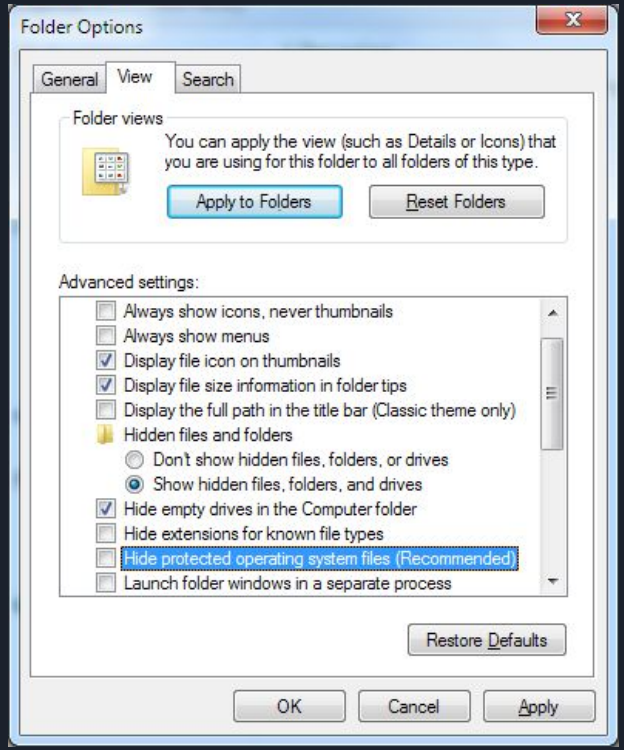


Super Hidden Files

Go back to the desktop and you'll see that... it's still not there?

Yes, that's because something else was done to it. It has system attributes. Go back to Folder Options and uncheck Hide Protected Operating System Files

You should now see the photos!



Making Super Hidden Files

Its pretty easy, but you have to use a command line tool called attrib.

The command (which must be run as administrator) is

Attrib filename +s +h

+s means make it a system file

+h means make it a hidden file

To convert a file back to normal, do attrib filename -s -h

You’re now a certified h4xx0r!